

ABSTRACT OF THE DISCLOSURE

A video source device includes a cipher unit. The cipher unit includes a block cipher and a stream cipher. The video source device uses the block cipher to generate at least one cipher key for use by the stream cipher to generate cipher bits for ciphering video to be transmitted to a video recording device. The video source device further provides n bits of copy control information to the video recording device. The video source device incorporates the n-bit copy control information as part of an initialization value, and initializes a register of a round function of the block cipher with the initialization value. The video recording device also includes a cipher unit of like kind, and operates the block and stream ciphers in like manner to decipher the ciphered video received from the video source device. Upon receiving the n-bit copy control information, the video recording device also forms an initialization value and initializes a corresponding register of the corresponding round function of its block cipher. Accordingly, protection is provided to the copy control information.

DECEMBER 10, 2000